# Cyber: Data, Insurance Trends, and Model Risk Update

Midwest Actuarial Forum—March 29, 2024

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

American Academy of Actuaries

# About the Academy


The American Academy of Actuaries is a 20,000-member professional association whose mission is to serve the public and the U.S. actuarial profession. For more than 50 years, the Academy has assisted public policymakers on all levels by providing leadership, objective expertise, and actuarial advice on risk and financial security issues.

The Academy also sets qualification, practice, and professionalism standards for actuaries in the United States.

For more information, please visit:
**www.actuary.org**

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Antitrust Notice



- The presenters' statements and opinions are their own and do not necessarily represent the official statements or opinions of the Actuarial Board for Counseling and Discipline (ABCD), Actuarial Standards Board (ASB), any boards or committees of the American Academy of Actuaries, or any other actuarial organization, nor do they necessarily express the opinions of their employers.
- The Academy operates in compliance with the requirements of applicable law, including federal antitrust laws. The Academy's antitrust policy is available online at https://www.actuary.org/content/academy-antitrust-policy.
- Academy members and other individuals who serve as members or interested parties of any of its boards, councils, committees, etc., are required to annually acknowledge the Academy's Conflict of Interest Policy, available online at https://www.actuary.org/content/conflict-interest-policy-1.

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Agenda



Cyber Risk Toolkit—Samuel Tashima, MAAA, FCAS

Cyber Data—Isabelle McCullough, MAAA, ACAS

State of the Cyber Insurance Market and Recent Trends in D&O—Samuel Tashima, MAAA, FCAS

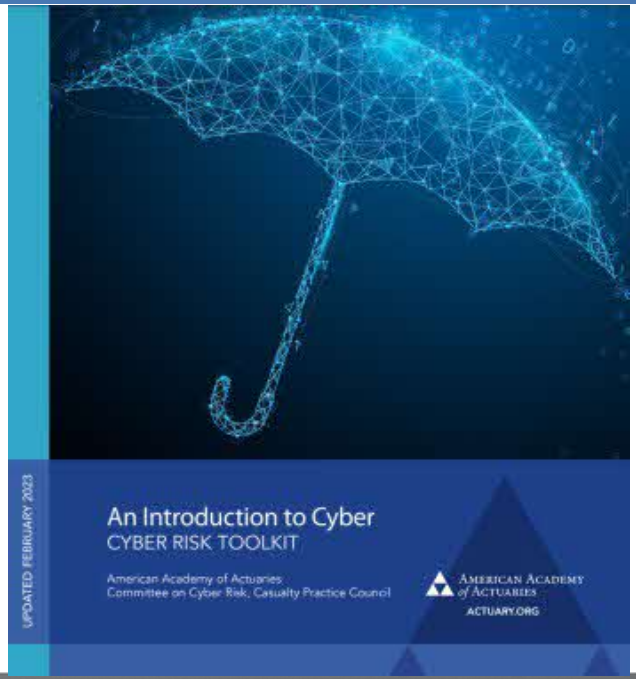
Cyber Risk Model Paper—Katie Koch, MAAA, FCAS

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Cyber Risk Toolkit



https://www.actuary.org/cybertoolkit




© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

American Academy of Actuaries

# Toolkit



- Developed by the Academy's Committee on Cyber Risk
- Papers in the toolkit address issues pertinent to cyber risk and exposure, which are now impacting most lines of business
- Intended to be a resource for interested readers of the general public, public policymakers, the actuarial profession, the insurance sector, and other stakeholders
- While each is a standalone paper, in total they offer a cohesive overview of the challenges posed in the cyber insurance market
- The toolkit will continue to be updated periodically to reflect new and emerging work from the committee

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Cyber Risk Toolkit



An Introduction to Cyber

Cyber Threat Landscape

Silent Cyber

Cyber Data

Cyber Risk Accumulation

Cyber Risk Reinsurance Issues

Ransomware

War, Cyberterrorism, and Cyber Insurance

Autonomous Vehicles and Cyber Risk

Personal Cyber: An Intro to Risk Reduction and Mitigation Strategies

Digital Assets and Their Current Roles Within Cyber Crime

Cyber Risk Resource Guide

**Upcoming topics:**
**Cyber Vendor Model Review**
**International Cyber Considerations**
**Personal Cyber Insurance Rating**

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

American Academy of Actuaries

# Cyber Data

Isabelle McCullough, MAAA, ACAS

Member, Committee on Cyber Risk

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

American Academy of Actuaries

# Cyber Data—Overview



Unlike other lines of business, where insurers typically have relied on vast amounts of premium, exposure, and claims data, cyber insurers have historically had a lack of adequate and relevant data to accurately evaluate risk.

While the amount of available data is growing, standard actuarial pricing models used for many other P&C lines do not work as well because insurers may be new to the cyber market and have limited data, or they have been writing cyber for years, but the exposure and risks continue to evolve. Same limitations apply to reserving for cyber as well.

**Cyber Risk Toolkit:** *Cyber Data*

https://www.actuary.org/sites/default/files/2023-02/4CyberData.pdf

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# What Is Cyber Data?



For the purposes of this discussion, in line with the Cyber Toolkit "Cyber Data" chapter, we will consider details related to cyber data as collected during the cyber insurance placement process and claims activity received from insureds that have purchased cyber insurance.

Other aspects not considered here include the following: security industry publications, threat intelligence feeds, vulnerability scans, professional services publications from law firms, and forensics providers.

**Cyber Risk Toolkit:** *Cyber Data*

https://www.actuary.org/sites/default/files/2023-02/4CyberData.pdf

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Cyber Data: Key Challenges

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Cyber Data: Key Challenges



Three main challenges that we will discuss:

- What data should be collected?
- Data collection needs vary over time
- What data can be reasonably collected?

- These challenges apply to both pricing & reserving, primary insurers & reinsurers
- Impacts of these challenges to different parts of the market may vary

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Challenge #1: What Data Should be Collected?



- Inconsistent management and analysis of cyber data across the insurance industry can create issues evaluating risk.
- Additional work is required to standardize the collected data to be able to analyze trends over time.
- These issues are broad and may apply both internally to individual insurers and externally as we look across the market.
- For example, within an insurance company, cyber may be written across multiple lines of business and global business units. Each unit may have different data collection standards and systems. This may present a challenge for the insurer to aggregate and use its own data for internal analysis.
- Similarly, where data is not standardized across the market, it may be difficult to aggregate data to analyze market-level trends (e.g., rate change, ransomware frequency).

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Challenge #1 (cont.): What Data Should Be Collected?



Examples of ways that insurers may overcome the data limitation/availability issues discussed:

- Collect additional data in the insurance placement process
- Supplement with publicly available data
- Consult with subject matter experts: CISO, IT Dept., CFO, Legal, Claims
- Leverage third-party cyber information providers for cyber threat intelligence, aggregation risk data
- Consider using data from technology firms in the underwriting process—diverse data including threat monitoring, outside-in / inside-out scanning, impact assessments

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Challenge #1 (cont.): What Data Should Be Collected?



More examples of how technology firms may enhance the data availability for the underwriting process:

- Firmographics: industry, revenue, employee count extracted from public sources
- Outside-in scanning: scan a company's network perimeter to identify their virtual supply chains and monitor security outcomes
- Inside-out scanning: sensors are installed in a company's network to scan its internal architecture to identify assets, device configuration, access points, etc.
- Threat monitoring: e.g. dark web scanning to uncover compromised organizations, new vulnerabilities
- Many more examples—refer to the Cyber Risk Toolkit—"Cyber Data" chapter

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

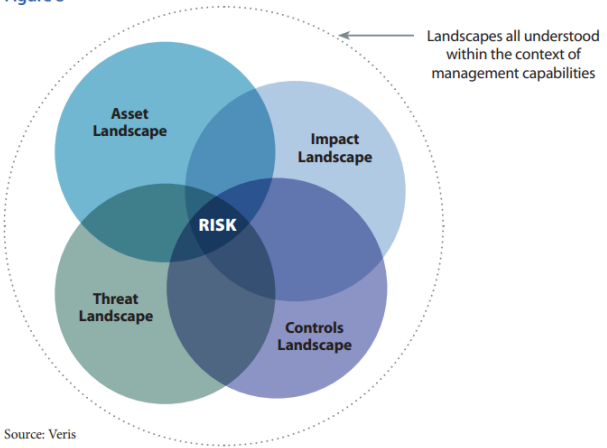
# Challenge #2: Evolution of Data Needs



Which data should be collected is changing over time for cyber risks

- As cyber exposure continues to evolve, the data needs of the market evolve with it. For example: ransomware questionnaires/supplements introduced when frequency picked up, security maturity/posture questions change over time as best practices evolve.
- Third-party vendors and data providers are working to fill in the gaps and stay on top of emerging data needs.
- Insurers can assess their own needs, internal data availability and capabilities against various vendors.

Figure 8




Source: Veris

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

American Academy of Actuaries

# Challenge #3: What Data Can Be Reasonably Collected?



Operational constraints must be considered. These include resource, budget, systems, etc.

Example considerations from the perspective of a primary insurer:

- Can the application be updated and/or extended?
- Will a longer, more robust application result in the collection of the required data?
- Do you usually receive your own application, or might you receive another insurer's application?
- Do competitors have shorter applications?
- Do policy or claims systems need to be updated? Are there downstream data impacts?
- Do multiple systems need to be updated in tandem (e.g., globally)?
- Are there filing implications beyond the application? For example, will the new data be used for determining eligibility or be used as a pricing input?

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Cyber Data:
# Practical Considerations for Pricing

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Small Commercial Cyber Pricing Considerations



We will consider small commercial cyber insurance in our first example to be standalone cyber for commercial insureds with $100m USD or less in gross revenues. Compared to the national account space, we expect:

- Higher volume submission flow
- Less complex risks
- More likely to require an admitted solution
- Lower GWP per policy
- Applicants less likely to have a dedicated risk manager, thorough understanding of cyber policy wording
- Applicants may be more likely to choose a carrier based solely on price
- May be more reliant on cyber insurance as a ‘security measure’ (i.e. less inclined to be proactive about their own security)
- Carriers may look to find ways to streamline the application, renewal processes in order to reduce expenses

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Small Commercial Cyber Pricing Considerations (cont.)



To deal with high submission volume and to reduce expenses, carriers may look to low-touch digital solutions, such as platforms or APIs for brokers to quote. May add complexity to system updates required for enhanced data collection.

Carriers may also look to streamline the renewal processes. One example is that insurers may collect less data at renewal than on a new business application. As cyber risk is constantly evolving, there may be more tradeoff between streamlining renewals and collecting important data on the risk (Challenge #2).

Renewals may be processed further in advance for small business (e.g., 60–90 days or more before inception). This may make it more challenging for carriers to react in a timely manner to collect new or enhanced data necessary for the underwriting process.

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Reinsurance Pricing Considerations



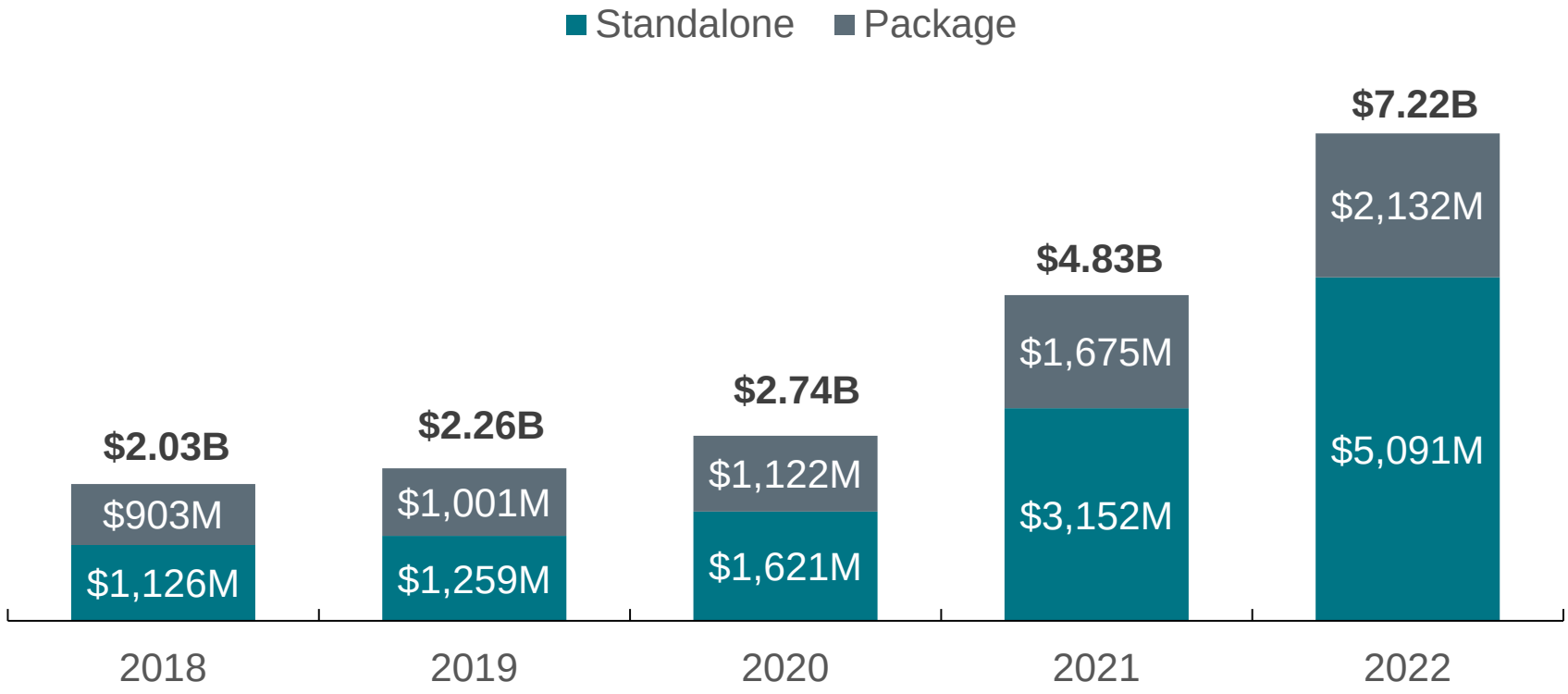
- Generally, exposure modeling is a part of the cyber reinsurance pricing process.
- Submissions include a risk bordereaux and may also include the applicants own raw modeling file. This is especially helpful where the format of the modeling files received are like the format needed for the reinsurer's internal model or vendor model.
- Anecdotally, data quality and completeness may vary significantly by market and even between insurers of similar size and market share.
- Missing or incomplete data may include coverage level detail (e.g., sub-limits), industry, revenues.
- Assumptions may be used in the modeling process where data is missing or incomplete.

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Cyber Insurance Landscape and Recent Trends

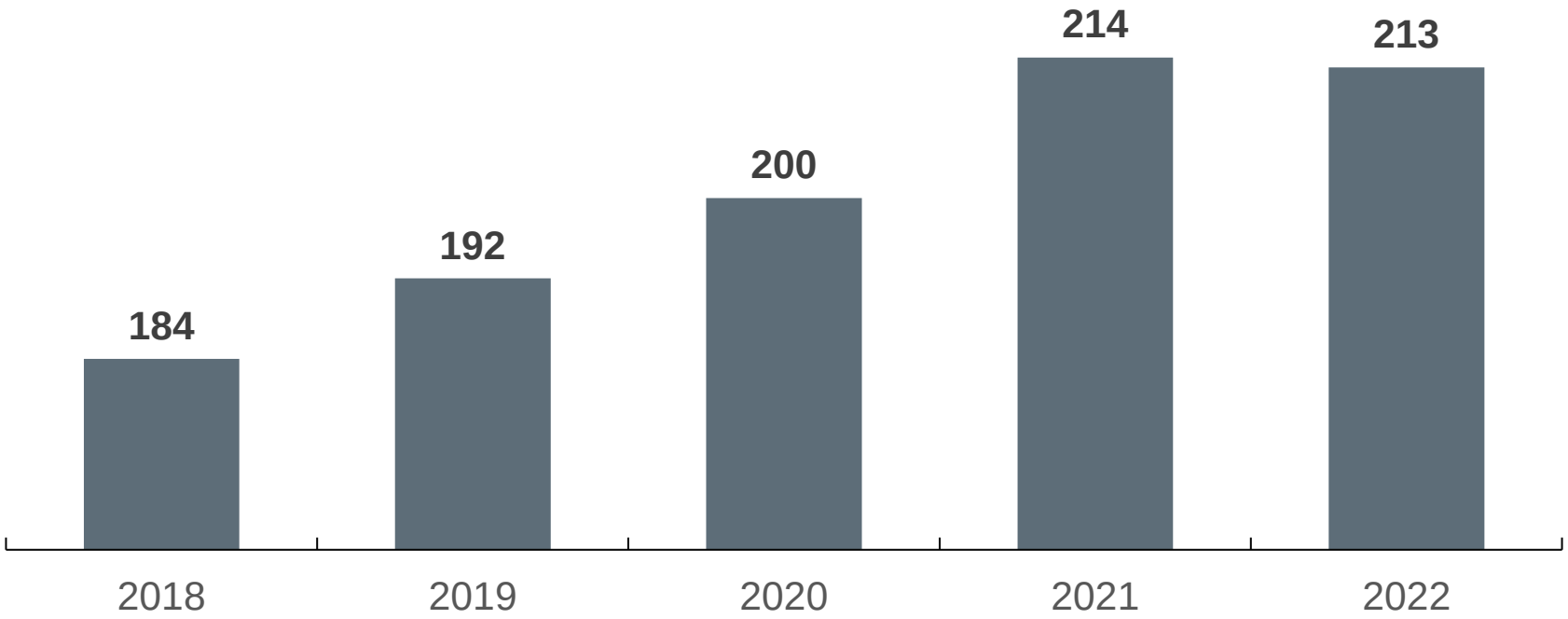
Sam Tashima, MAAA, FCAS
Vice Chairperson, Committee on Cyber Risk

# U.S. Cyber Direct Written Premiums | 2017–2022



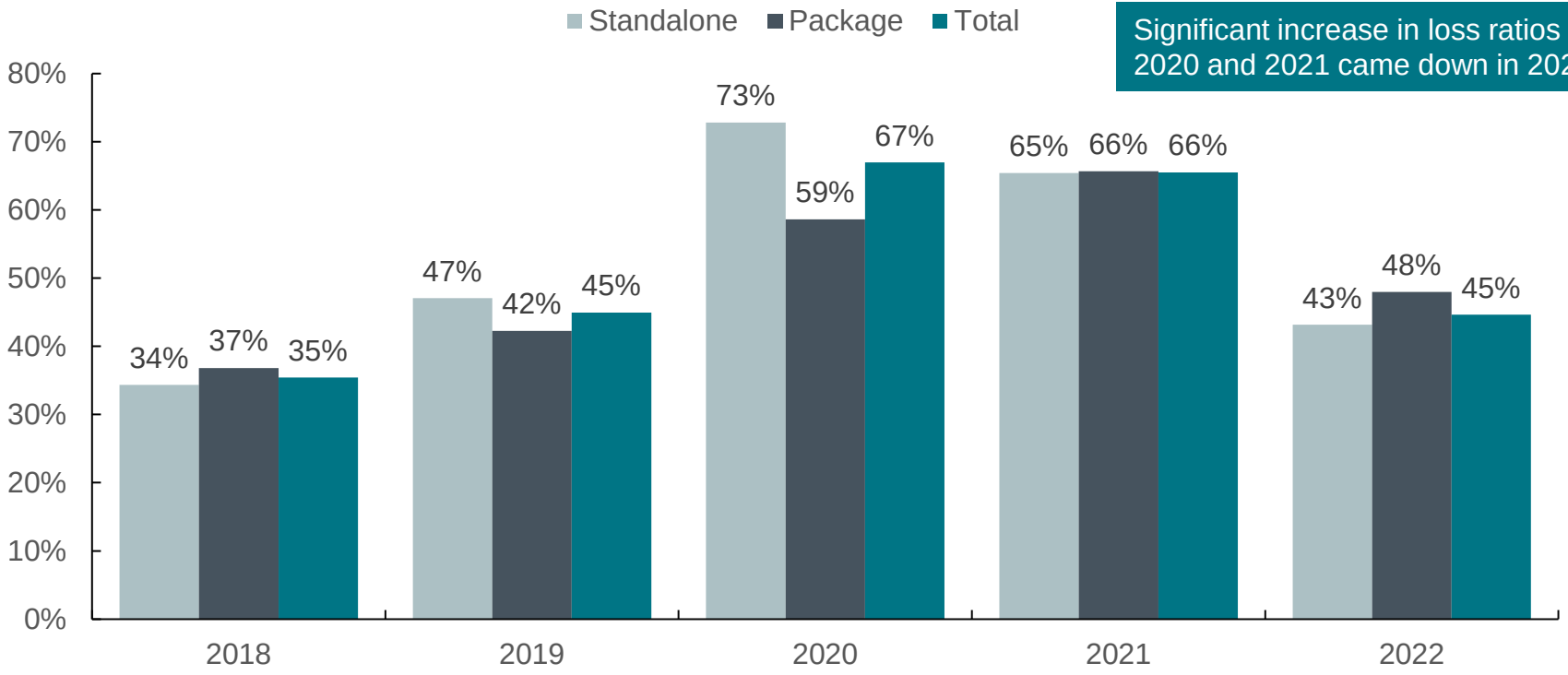

Source: Aon's U.S. Cyber Market Update: 2022 U.S. Cyber Insurance Profits and Performance

# Number of U.S. cyber insurers | 2017–2022




Source: Aon's U.S. Cyber Market Update: 2022 U.S. Cyber Insurance Profits and Performance

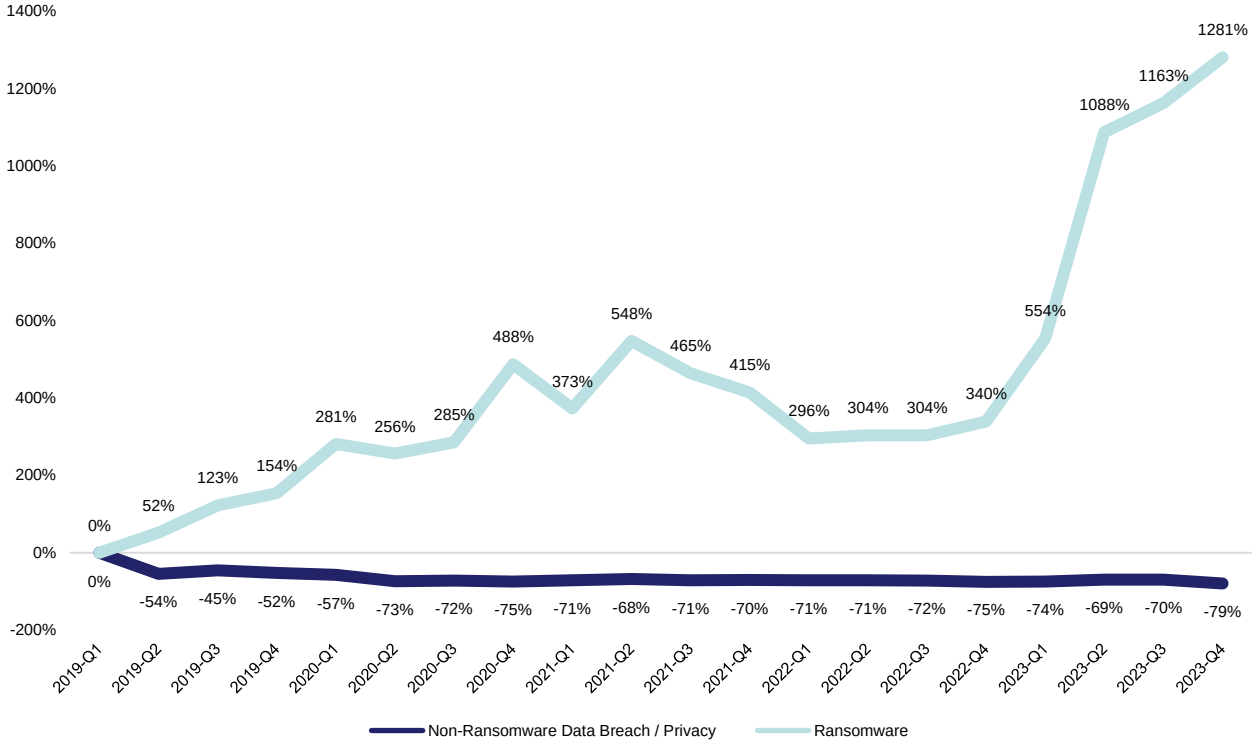
# U.S. Cyber Loss Ratio | 2017–2022




Significant increase in loss ratios for 2020 and 2021 came down in 2022

Source: Aon's U.S. Cyber Market Update: 2022 U.S. Cyber Insurance Profits and Performance

# Cyber Incident Rates Indexed to Q1 2019



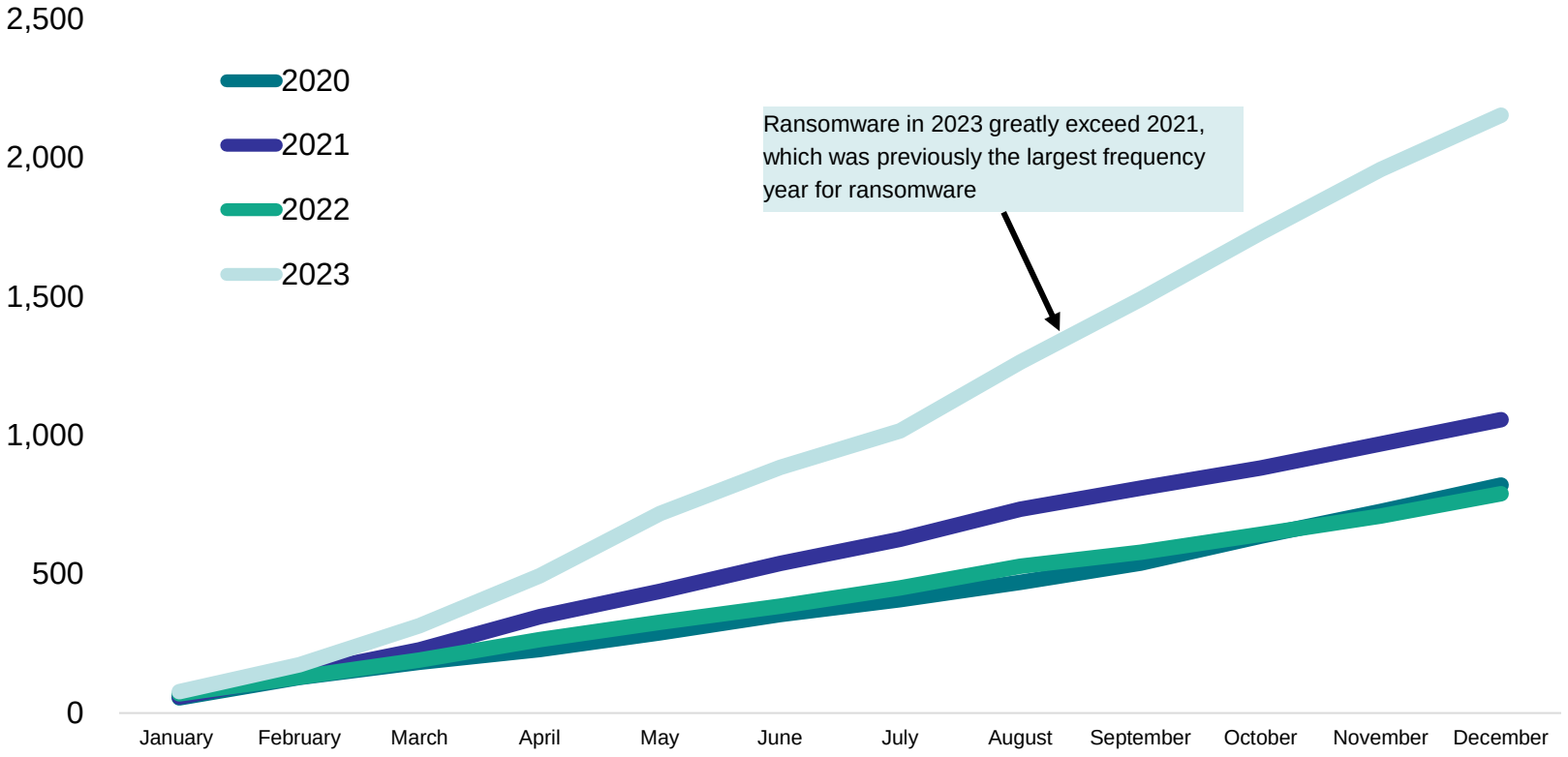

**Key Observations:**

- Ransomware activity has continued to **accelerate through Q4 2023**
- **Ransomware Events are up 1,281%** from Q1 2019 to Q4 2023
- Compared to Q3 2023:
  - Ransomware Events are up 9%
  - Non-Ransomware Data Breach/Privacy Events are down 32%
- The most commonly impacted industries by Ransomware in Q4 2023 were:
  - Business Professional Services
  - Manufacturing
  - Healthcare
  - Real Estate / Construction
  - Education
  - Public Entities

Source: Risk Based Security, analysis by Aon. Data as of 1/1/2024; Claim count development may cause these percentages to change over time

Proprietary & Confidential: The content, analysis and commentary included herein are understood to be the intellectual property of Aon. Further distribution, photocopying or any form of third-party transmission of this document in part or in whole, is not permitted without the express, written permission of Aon.

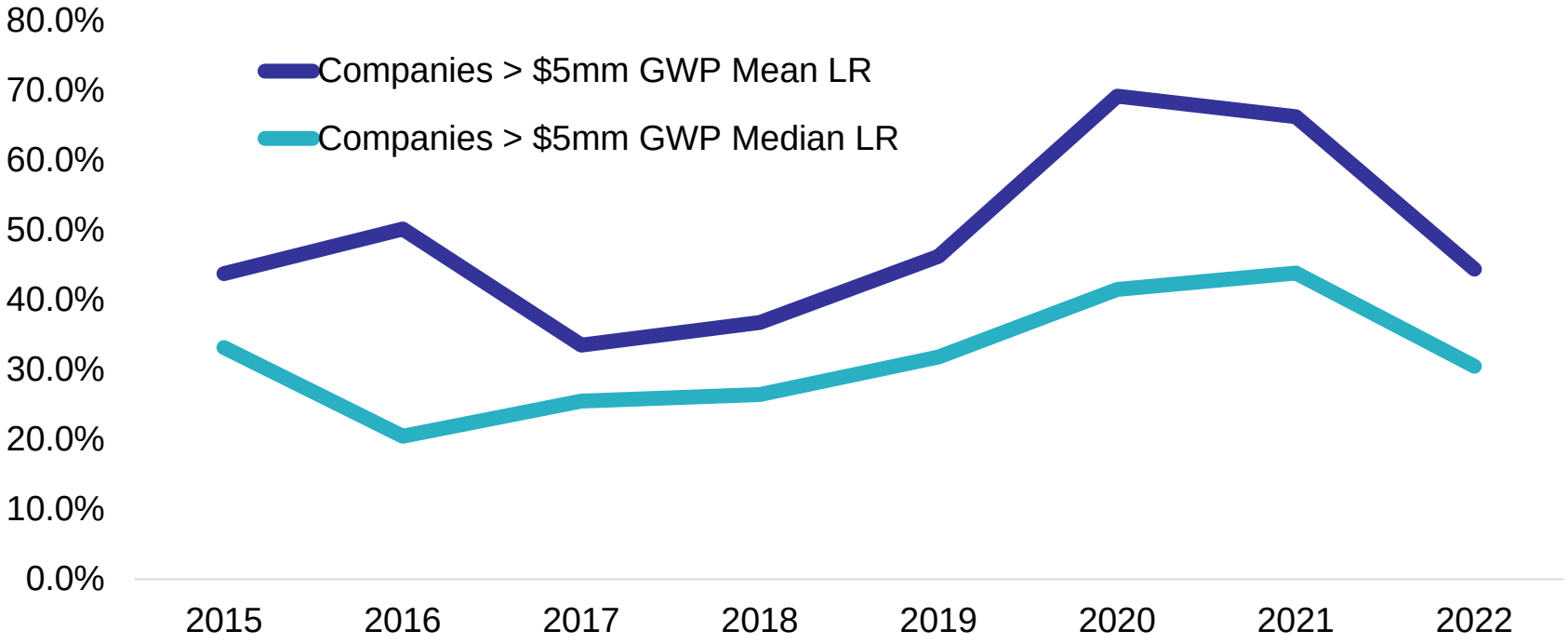
# Cumulative Ransomware Frequency Growth by Month




Source: Risk Based Security, analysis by Aon. Data as of 1/1/2024; Claim count development may cause these figures to change over time

Proprietary & Confidential: The content, analysis and commentary included herein are understood to be the intellectual property of Aon. Further distribution, photocopying or any form of third-party transmission of this document in part or in whole, is not permitted without the express, written permission of Aon.

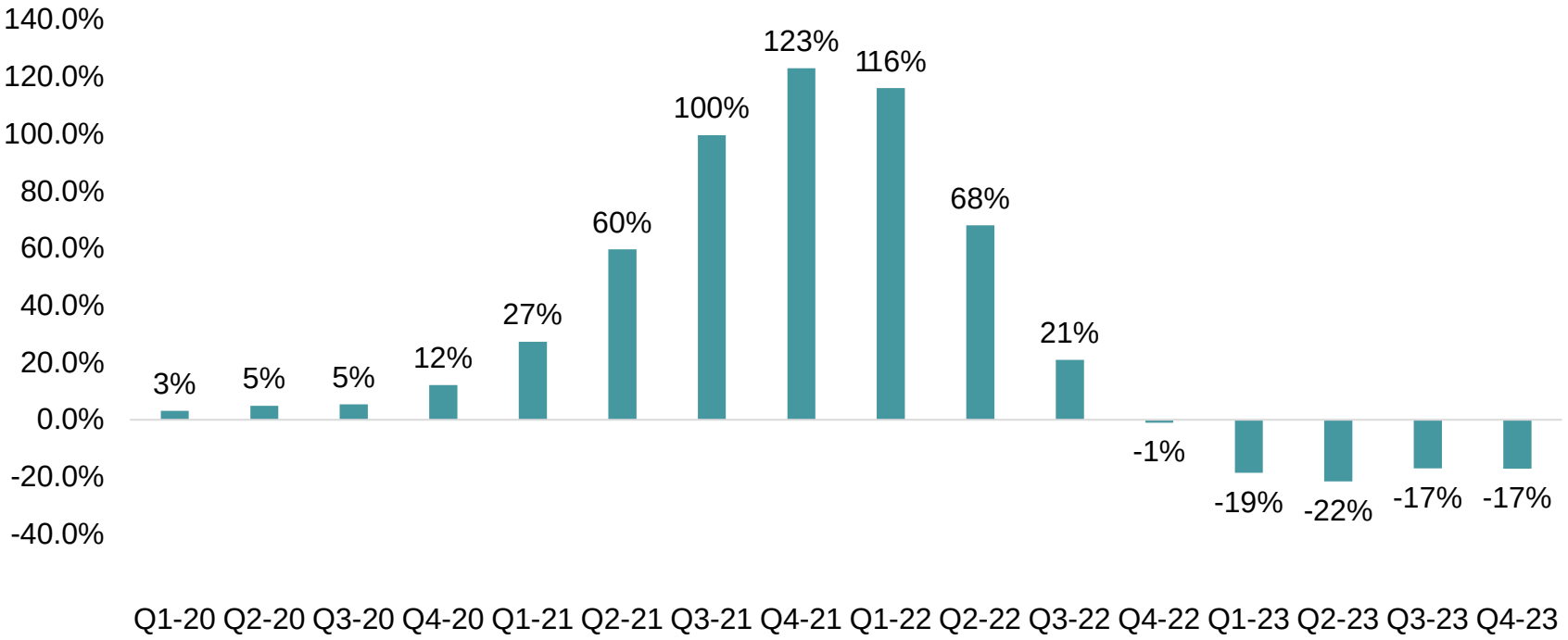
# U.S. cyber loss ratio, gross written premium (GWP) > $5M | 2015–2022




Source: Aon's U.S. Cyber Market Update: 2022 U.S. Cyber Insurance Profits and Performance

# How are markets responding?

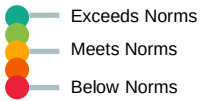
# 2020–2023 cyber premium changes by quarter
## Average year-over-year change (same clients)




Source: Aon's E&O and Cyber Market Review – Q1 2024

# Cyber Liability Q1 2024 Market Dynamics

| | |
|---|---|
| **Pricing**<br>**Primary: (Consistent)**<br>**Excess: (Consistent to Decreasing)** | |
| **Capacity/Limit (Improving)** | |
| **Underwriting / Process (Rigorous / Consistent)** | |
| **Retentions (Consistent)** | |
| **Coverages (Consistent to Restricting)** | |
| **Claims & Loss (Increased Frequency)** | |




**Overall**

**Buyer friendly market conditions was the theme of the cyber market in 2023. Greater competition and more capacity drove incumbent insurers to maintain their renewals and potentially expand their participation. As pricing continued to decelerate for excess layers, more insureds have opted to purchase additional limits, using data and analytics to support their decision.**

**Risk differentiation will remain important to insurers, and insurers will price for that differentiation accordingly. Insurers still seek a significant amount of underwriting data and best-in-class network security controls, but underwriters now also focus on understanding and ensuring best-in-class privacy controls.**

**A Look Ahead**

- Looking ahead – depending on the class of business, year-over-year improvement of controls, and previous market corrections – **Q1 2024 should yield further buyer-friendly market results**, with the majority of the savings coming from the high excess layers.
- As we look forward to what may be a volatile market over the next 3-5 years, **identifying the right long-term insurer who understands your risk, has a proven track record of paying claims and is willing to customize policy wording to address your exposures and incident response strategies is critical**.
- **Pricing for large market companies will stabilize in Q1 of 2024**. Competition and new capacity in the primary middle market segment as well as the national account excess layers segment continue to drive pricing down.
- **Systemic risk** is a top concern for insurers. They continue to evaluate, scrutinize, and in some instances restrict coverage offered for critical infrastructure, systemic and/or correlated events, and war. Certain insurers restrict coverage on either a generalized or event specific basis.
- **Privacy related losses are mounting, and they are severe.** Insurers are increasing underwriting scrutiny related to privacy exposures and data collection (including biometric information, pixel tracking and new privacy/consumer protection regulations).

# How are enterprise insureds responding?

1. Increasing limits given the stabilizing market
2. Turning to higher SIRs and limit adequacy – emphasizing catastrophic coverage
3. Focus on terms & conditions
   (LMA wording for Cyber War Exclusion)
4. Prioritizing long term program goals
5. Focusing on top reasons for insurer declinations
6. Leveraging captive insurance programs

# SEC Disclosures and Related Matters

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

American Academy of Actuaries

# SEC 8-K Disclosure Laws



Effective 12/18/2023

The registrant must file the Item 1.05 Form 8-K within four business days of its determination that the incident is material.

https://www.huntonprivacyblog.com/2023/12/18/sec-cyber-8-k-rules-effective-today/

https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# SEC 8-K Example Disclosure



**Item 1.05. Material Cybersecurity Incidents.**

On February 21, 2024, UnitedHealth Group (the "Company") identified a suspected nation-state associated cyber security threat actor had gained access to some of the Change Healthcare information technology systems. Immediately upon detection of this outside threat, the Company proactively isolated the impacted systems from other connecting systems in the interest of protecting our partners and patients, to contain, assess and remediate the incident.

The Company is working diligently to restore those systems and resume normal operations as soon as possible, but cannot estimate the duration or extent of the disruption at this time. The Company has retained leading security experts, is working with law enforcement and notified customers, clients and certain government agencies. At this time, the Company believes the network interruption is specific to Change Healthcare systems, and all other systems across the Company are operational.

During the disruption, certain networks and transactional services may not be accessible. The Company is providing updates on the incident at https://status.changehealthcare.com/incidents/hqpjz25fn3n7. Please access that site for further information.

As of the date of this report, the Company has not determined the incident is reasonably likely to materially impact the Company's financial condition or results of operations.

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# SEC 10-K Disclosure Laws



New Item 106-Cybersecurity Risk Management and Governance

For the 10-K disclosures, disclosures will be due with annual reports for fiscal years ending on or after December 15, 2023.

Item 106 and Item 16K require registrants to describe their processes, if any, for assessing, identifying, and **managing material risks from cybersecurity threats, as well as whether any risks from cybersecurity threats**, including as a result of any previous cybersecurity incidents, **have materially affected or are reasonably likely to materially affect them**. The new rules include a non-exclusive list of disclosure items registrants should provide based on their facts and circumstances.

https://www.sec.gov/corpfin/secg-cybersecurity

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Cyber and Privacy Issues Can Lead to D&O Losses



## Securities Class Actions

### Yahoo!
- (03/02/18) $80M Securities
- (01/04/19) $29M Derivatives

### Equifax
- (02/13/20) $149M Securities

### SolarWinds
- (10/28/22) $26M Securities

### Alphabet
- (02/05/24) $350M Securities

## SEC Charges

### Control Failures
- First American Financial Corporation—(06/15/21) $487,616
- Morgan Stanley—(09/20/22) $35M
- SolarWinds—(10/30/23)

Fraud, internal control failures, misleading investors

### Misleading Investors
- Yahoo!—(04/24/18) $35M
- Pearson—(08/16/21) $1M
- Blackbaud—(03/09/23) $3M

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Cyber Model Risk Paper

Katie Koch, MAAA, FCAS

Member, Committee on Cyber Risk

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

American Academy of Actuaries

# Purpose



An effort to identify and explore features of a sample of models available in the cybersecurity market

A high-level review of eight models in the cyber risk space

Motivated by the proliferation of models and services designed to address various aspects of cyber risk quantification

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Disclaimer



The selection or exclusion of specific models and vendors reflected in the paper should not be interpreted as an endorsement of the reviewed models. The paper reflects a sample from a wide variety of models available in the cybersecurity market and it is likely there are many useful models that the committee was unable to review. The intended purpose and degree of sophistication of cyber risk quantification models varies widely.

The American Academy of Actuaries is not promoting or advertising for any particular model. Any entity selecting a cyber risk model for use is responsible for due diligence.

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Models Reviewed



The committee conducted direct discussions with the vendors, including for the following four models:

*Models with vendor interview*

CyberCube

Cyence Cyber Risk Model

Kovrr Quantum Cyber Risk Quantification

MMC Cyber Blue(i) Model

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Models Reviewed (continued)



The committee summarized information based exclusively on publicly available information at the vendors' websites for the following four models:

*Models without vendor interview*

Bitsight for Cyber Insurance

Experian

ISS ESG Cyber Risk Score

RiskLens Rapid Risk Assessment

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Summary of Vendor Models (with Interviews)



| | Kovrr | CyberCube | Cyence | MMC |
|---|---|---|---|---|
| **Model Purpose** | To enable (re)insurers to predict and price cyber risk | To combine single risk underwriting and aggregation risk modeling to help insurers measure the financial impact of emerging cyber risks | To produces loss estimates for seven different cyber event types | To capture the potential impact on insureds of losses from the three 'perils' that are commonly covered by commercial cyber insurance policies: (1) privacy data breach, (2) business interruption, and (3) ransom. |
| **Model Data Source** | Data partnerships with third party databases | Indicated having access to telemetry data from cybersecurity firm, Symantec, and other data partners | Reportedly uses a wide range of inputs and data sources with data curated through data mining, natural language processing, machine learning, pattern matching, and behavioral analysis | Industry data aquired by, subscription, third parties reflecting past incidents, and on proprietary anonymized client data. |
| **Model Accesibility** | Kovrr is reportedly active in Israel, Europe, US and Australia. | CyberCube lists among its clients, 17 out of the 30 largest cyber insurers, four out of the 5 largest reinsurers, and 16 out of the top 50 cyber insurance brokers, in the world. | Several different platforms are reportedly available for various users | Intended to be used by insurance brokers and consultants to recommend the appropriate levels of insurance. |

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Summary of Vendor Models (public sources)



Bitsight for Cyber Insurance

- Underwriting tool intended to provide transparency into the cyber risk profile of an insured

Experian Cyber Risk Model

- The intended purpose is to improve the underwriting process for cybersecurity insurance policies and identify business vulnerabilities
- Intended to incorporate the human element of cyber risk

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Summary of Vendor Models (public sources) (cont.)



ISS ESG Cyber Risk Score

- Intended purpose includes identifying and managing cyber risk across an investment portfolio

RiskLens Rapid Risk Assessment

- Intended purpose is to quantify an entity's loss exposure and rank risks by probable impact, which can facilitate identification of emerging threats and prioritization of cybersecurity efforts

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

# Thank you



Questions?

For more information, contact:
Rob Fischer, casualty policy analyst
fischer@actuary.org

© 2024 American Academy of Actuaries. All rights reserved.
May not be reproduced without express permission.

American Academy of Actuaries